Cloud Extractor を使用した
iCloud Applications
抽出ガイド

Ver. 1.0

目次

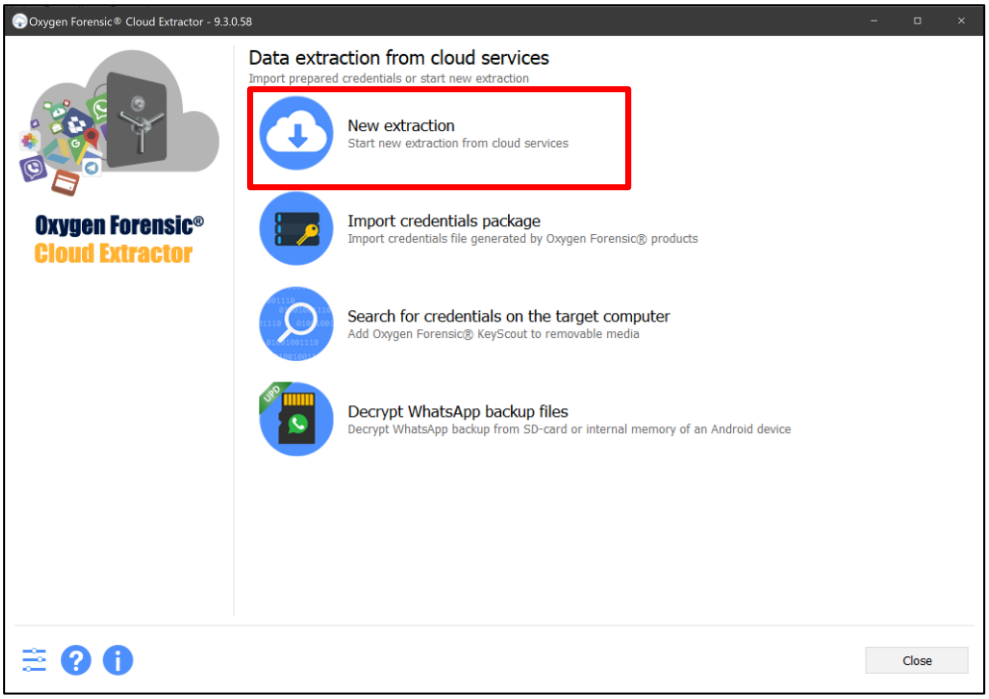
1　前提

本手順で取得出来るデータは、iCloud Drive にアップロードされたアプリケーションのバックアップデータが対象となります。

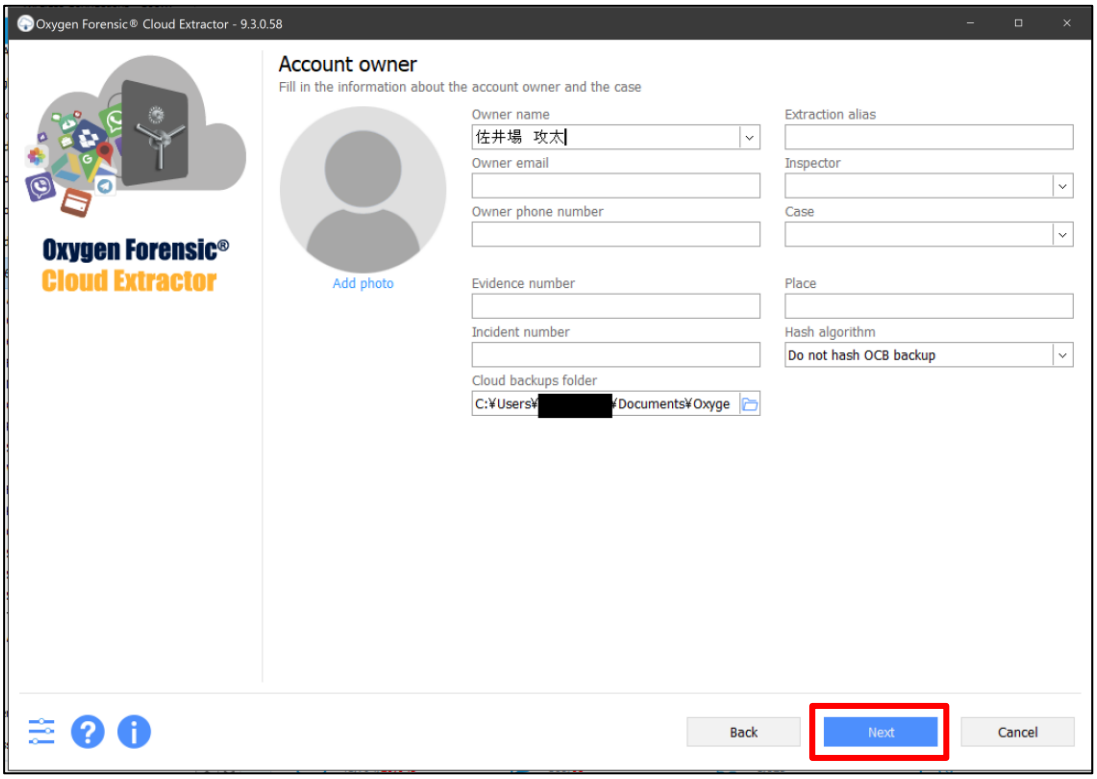
また、データ取得時にスマートフォンに送信される AppleID 確認コード(パスコード)の確認が必要になりますので、ネットワークに接続されたバックアップ対象のスマートフォンをお手元にご用意ください。

2　抽出

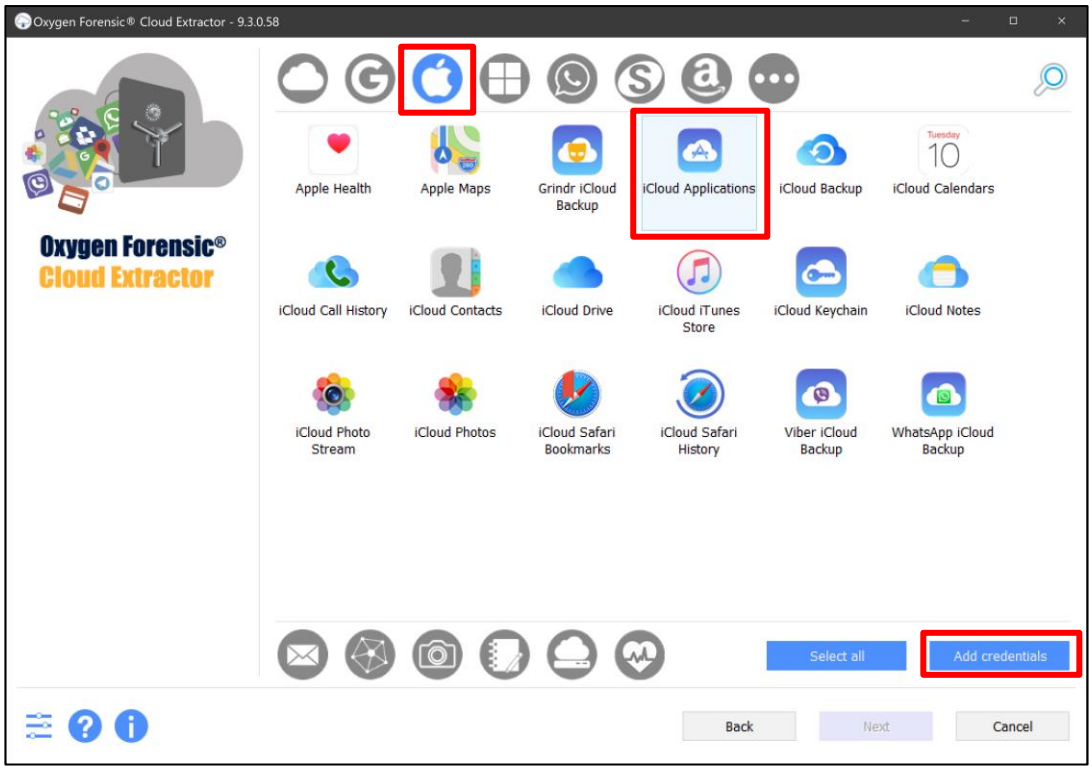
1.　Oxygen Forensic Cloud Extractor を起動し、[New extraction]をクリックします。



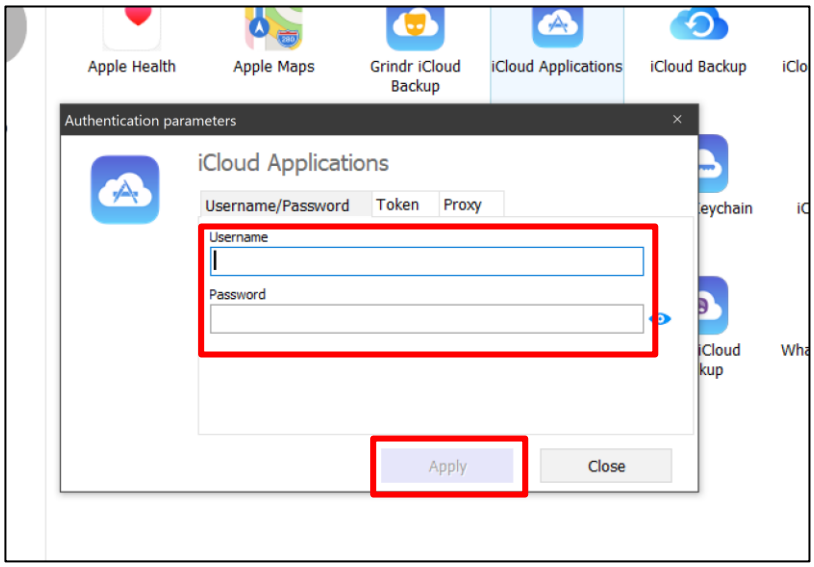
2. 抽出対象のデバイスの持ち主情報を入力し、[Next]をクリックします。



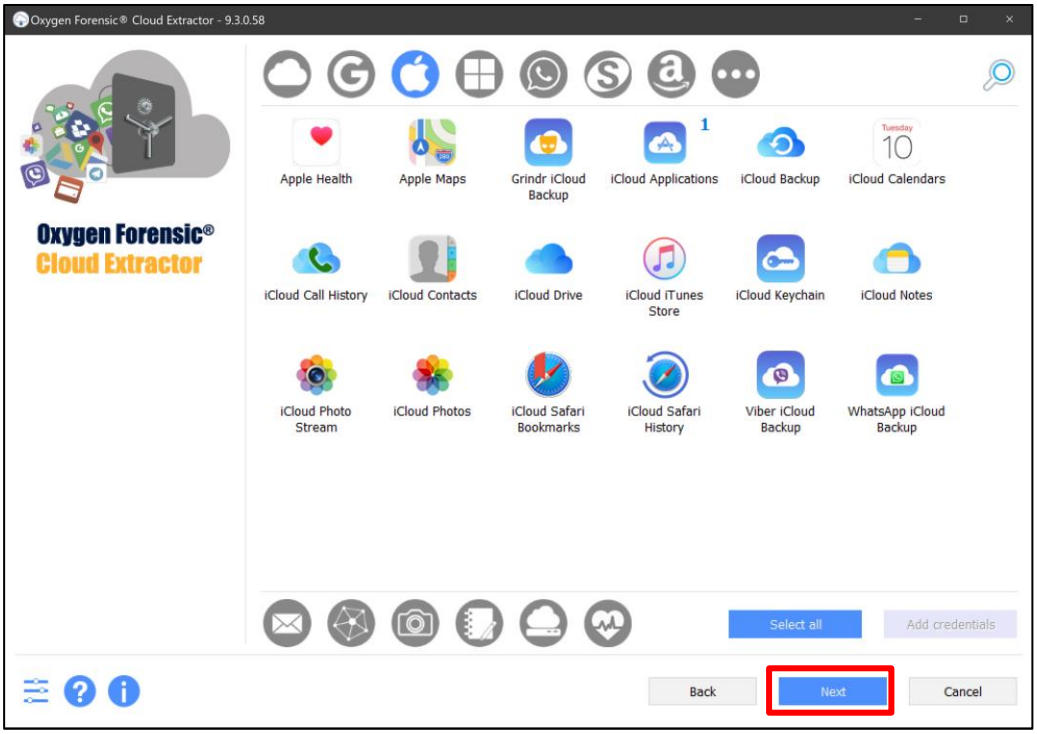
3. 抽出するアプリケーションを選択する画面では、Apple マークをクリックし、[iCloud Applications]を選択してください。選択後、[Add credentials]をクリックしてください。



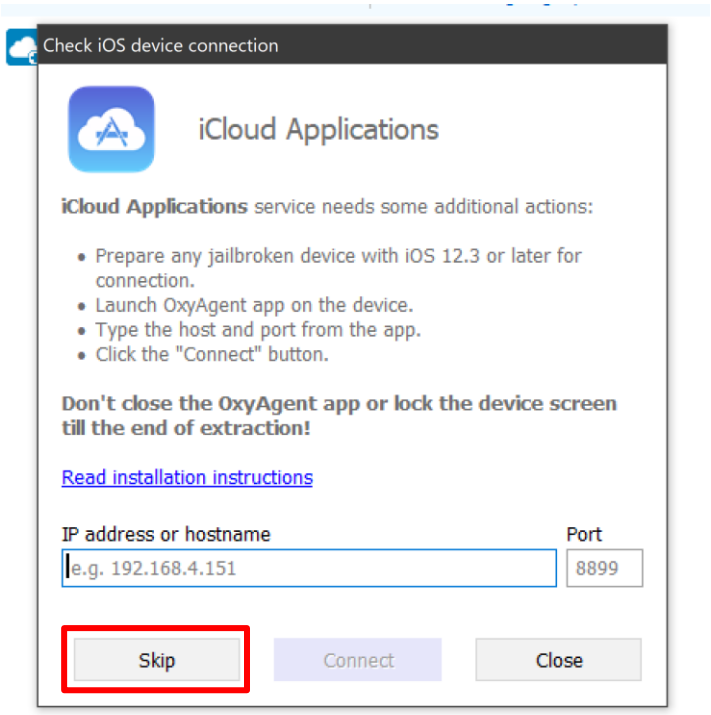
4. 『Authentication parameters』ウィンドウが表示されますので、AppleID の Username と Password を入力してください。入力後は[Apply]をクリックしてください。



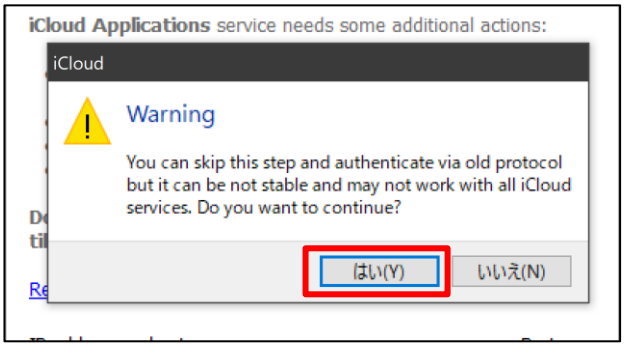
5. [Next]をクリックしてください。



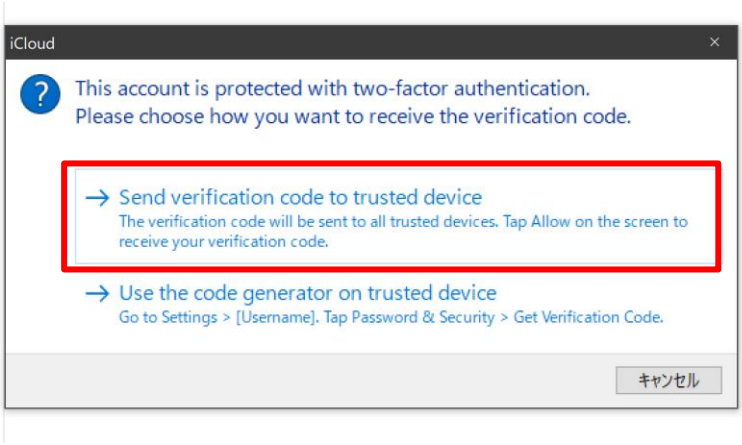
6. 『Check iOS device connection』という画面が表示されますが、今回はこれらの機能を使用せずに行う抽出を解説しますので、[Skip]をクリックしてください。



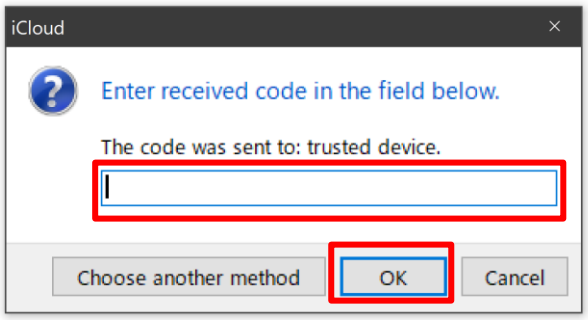
7. 『Warning』が表示されますが、[はい]をクリックしてください



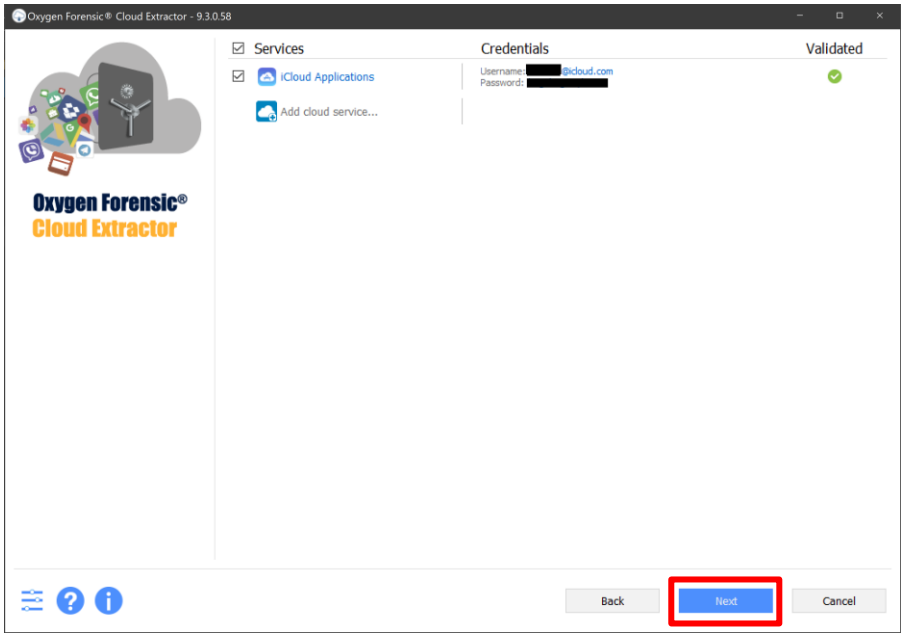
8. [Send verification code to trusted device]をクリックしてください。



9. スマートフォン側で AppleID 確認コードが表示されますので、その数字を「Enter received code in the field below.」と表示されているウィンドウに入力して[OK]をクリックしてください。

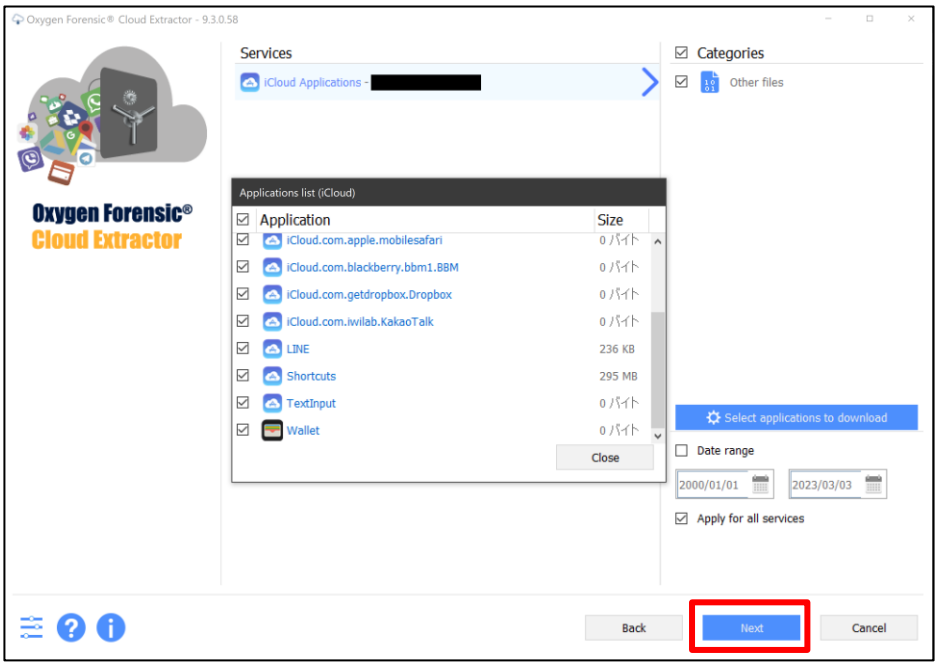


10. 無事に認証が完了しますと、下図の画面になりますので[Next]をクリックしてください。

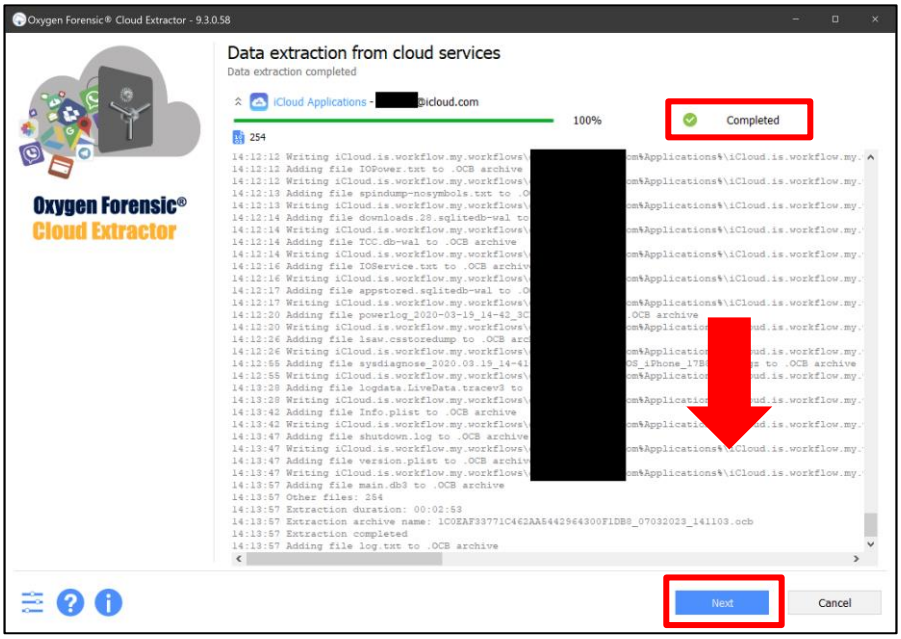


11. 抽出対象範囲の設定画面が表示されます。設定が完了しましたら、[Next]をクリックして抽出を開始してください。

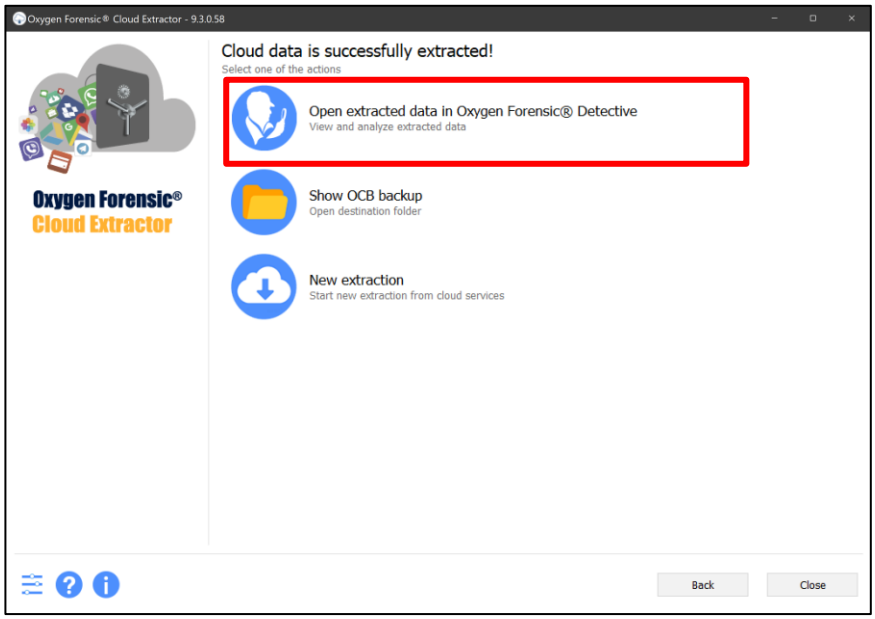
    [Select applications to download]をクリックすると、抽出対象の Application を絞り込むことが可能です。また、Categories からファイルの種類、Date range からデータの日付範囲を設定可能です。



12. 下図のような画面に遷移し、抽出が開始されます。完了すると「Completed」と表示されますので、[Next]をクリックしてください。

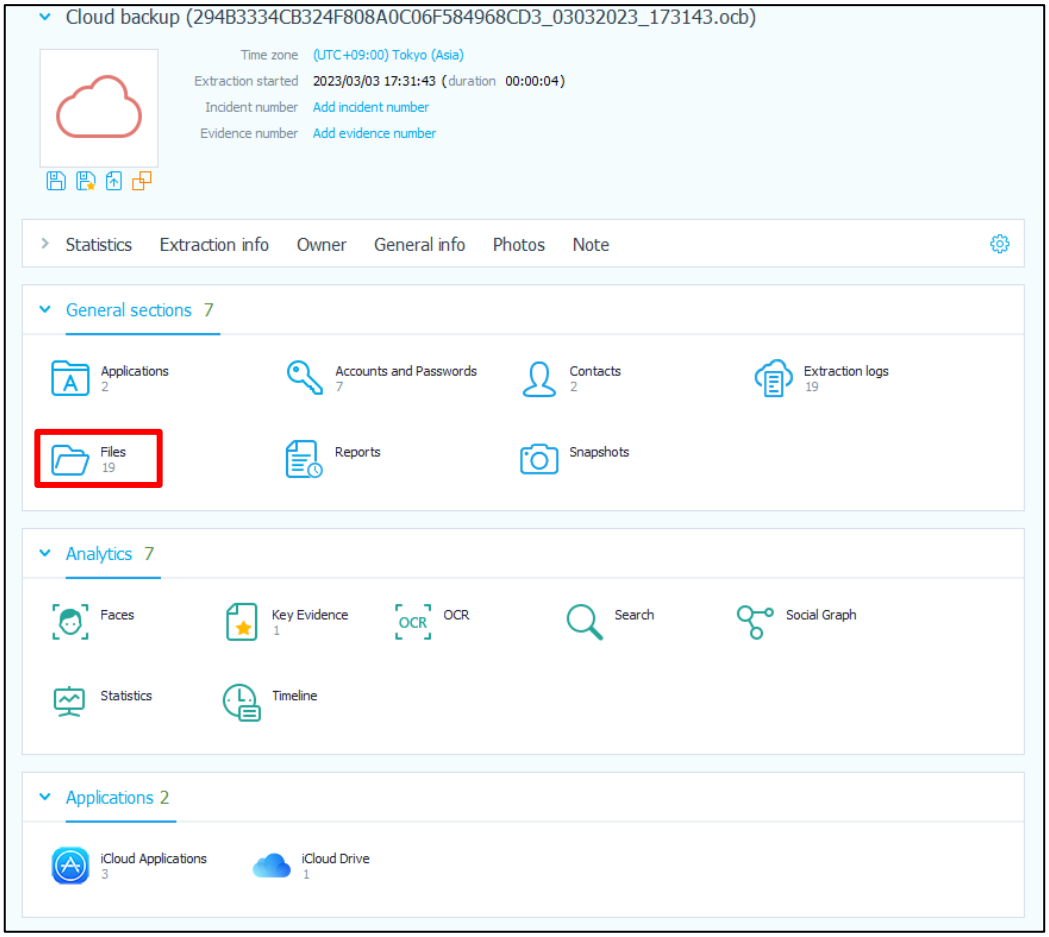


13. 抽出が完了しましたら、下図の画面が表示されるまで[Next]をクリックしてください。下図の画面が表示されましたら、[Open extracted data in Oxygen Forensic Detective]をクリックします。

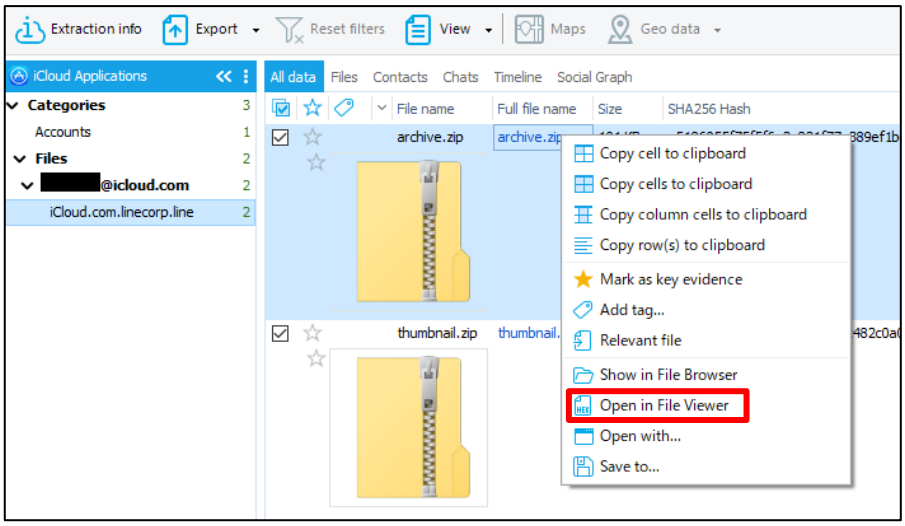


3 解析

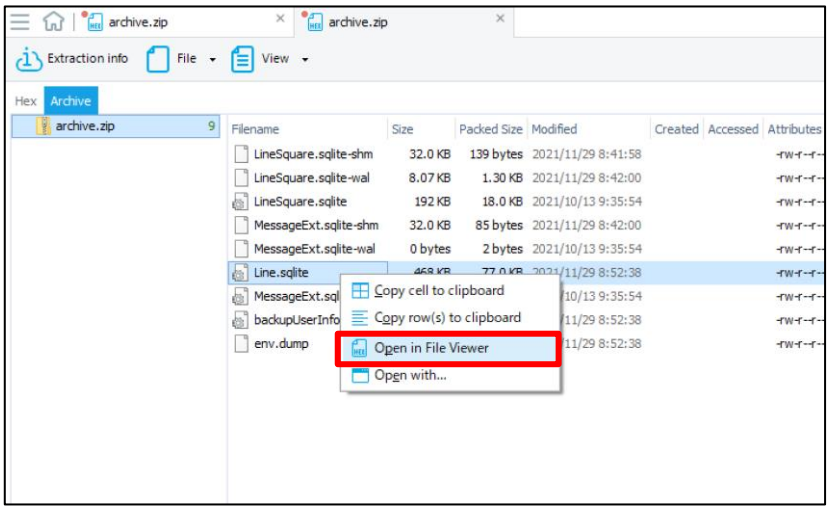
1. 抽出したデータを Oxygen Forensic Detective で解析すると、下図のように表示されます。



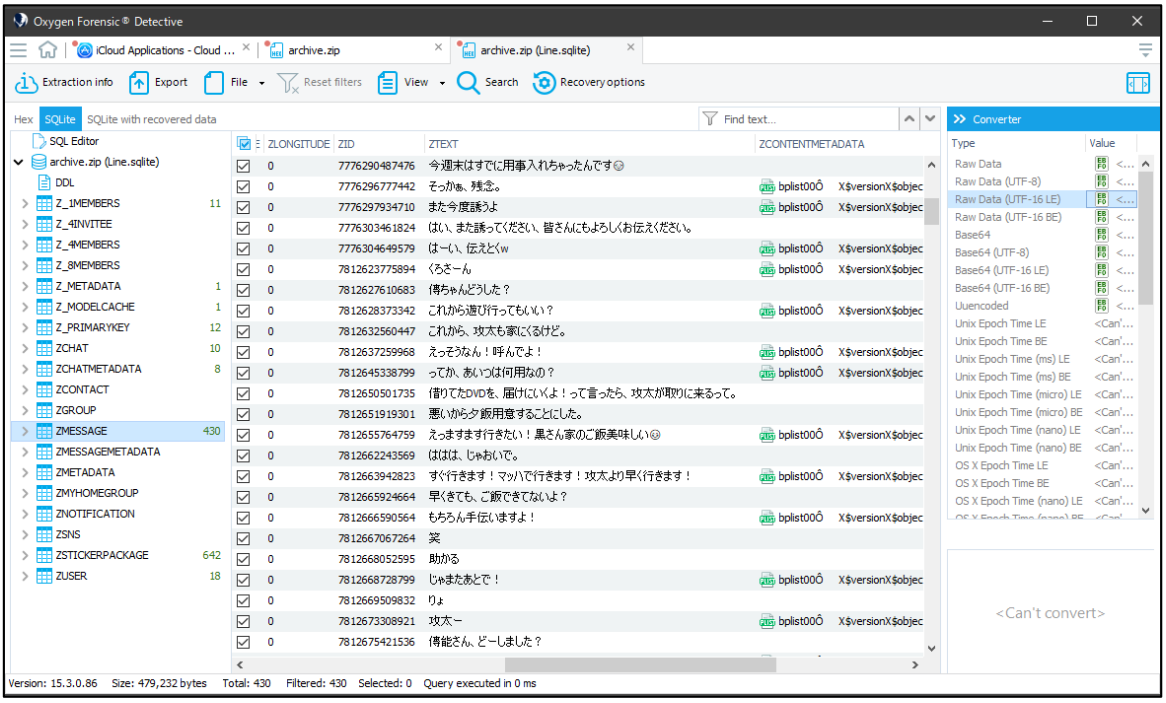
2. Files セクションに遷移し、バックアップファイルを右クリックしてオプションメニューを開き、[Open in File Viewer]をクリックしてください



3. この例では、バックアップファイルの中に DB ファイルが格納されています。DB ファイルの上で右クリック→[Open in File Viewer]をクリックします。



4. このように、バックアップファイルの中に格納されていた DB ファイルを開くことが出来ます。



改訂履歴

版数	発行日	改訂履歴
Ver. 1.0	2023 年 03 月 06 日	初版発行